**Schools’ Accountancy Team**

FAQs: PCI DSS

This document should be used in conjunction with the [Suffolk Scheme for the Financing of Schools.](http://www.suffolklearning.co.uk/leadership-staff-development/schools-accountancy/finance-regulations)

|  |
| --- |
| **USEFUL LINKS:** |
| **National:**[PCI DSS Security Standards](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)[PCI DSS FAQs](https://www.pcicomplianceguide.org/pci-faqs-2/)[Self Assessment Questionnaire B](https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-B.pdf?agreement=true&time=1548415465604) | **Schools’ Accountancy Team:**[Finance Regulations](https://suffolklearning.com/wp-content/uploads/2021/07/PCI_DSS_Finance_Regulations_REVISED.docx)[LMS Document](https://suffolklearning.com/finance/schools-accountancy/lms/) [Certificate of PCI DSS Compliance](https://suffolklearning.com/wp-content/uploads/2022/01/PCI_DSS_Certificate_2022.docx) | **Schools’ Choice:**[Model Policy](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-model-policy.docx) [Model Procedures](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-model-procedures.docx) [Staff Declaration](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-staff-declaration.doc) [Staff Log](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-staff-log.doc) |
| **SCHOOL CIRCUMSTANCES:** | **ACTION REQUIRED:** |
| * doesn’t use ParentPay or another third-party organisation

*and** doesn’t accept/process card payments and has no stored account data
 | 1. Complete **Section A of the** [**Certificate**](http://www.suffolklearning.co.uk/cms/view_folder.asp?rootid=6&depth=4&level1=6&level1id=6&level2=3379&level2id=3379&level3=3384&level3id=3384&nextlevel=3560&folderid=3560) and send to sat@suffolk.gov.uk by 31 March
 |
| * uses ParentPay or another third-party organisation

*and** doesn’t accept/process card payments and has no stored account data
 | 1. Complete **Section B of the** [**Certificate**](http://www.suffolklearning.co.uk/cms/view_folder.asp?rootid=6&depth=4&level1=6&level1id=6&level2=3379&level2id=3379&level3=3384&level3id=3384&nextlevel=3560&folderid=3560) and send to sat@suffolk.gov.uk by 31 March
2. Obtain an **Attestation of Compliance** from the third-party organisation. These are usually published on their websites (annual task)
 |
| * doesn’t use ParentPay or another third-party organisation

*and** does one or more of the following:a) holds a PDQ Terminalb) handles/processes account/card datac) holds account/card data
 | 1. Complete **Section C of the** [**Certificate**](https://www.schoolsurf.suffolkcc.gov.uk/docs/unrestricted/Finance_Service/Financial_Management/Forms/index.aspx) and send to sat@suffolk.gov.uk by 31 March
2. Agree a **PCI DSS Policy** and arrange for regular reviews ([Model Policy](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-model-policy.docx) available)
3. Identify appropriate procedures and add written instructions to the school’s **Local Procedures Manual** ([Model Procedures](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-model-procedures.docx) available)
4. Require staff handling/processing account/card data to complete staff declarations ([Staff Declaration](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-staff-declaration.doc) template available)
5. All staff to sign as evidence of receipt of the PCI DSS Policy ([Staff Log](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-staff-log.doc) template available)
6. Complete the **PCI DSS** [**Self Assessment Questionnaire B,**](https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-B.pdf?agreement=true&time=1548415465604)the signed copy is retained in school (annual task)
 |
| **SCHOOL CIRCUMSTANCES:** | **ACTION REQUIRED:** |
| * uses ParentPay or another third-party organisation

*and** does one or more of the following:a) holds a PDQ Terminalb) handles/processes account/card datac) holds account/card data
 | 1. Complete **Section B and Section C of the** [**Certificate**](http://www.suffolklearning.co.uk/cms/view_folder.asp?rootid=6&depth=4&level1=6&level1id=6&level2=3379&level2id=3379&level3=3384&level3id=3384&nextlevel=3560&folderid=3560https://www.schoolsurf.suffolkcc.gov.uk/docs/unrestricted/Finance_Service/Financial_Management/Forms/index.aspx) and send to sat@suffolk.gov.uk by 31 March
2. Obtain an **Attestation of Compliance**from the third-party organisation. These are usually published on their websites (annual task)
3. Agree **a PCI DSS Policy** and arrange for regular reviews ([Model Policy](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-model-policy.docx) available)
4. Identify appropriate procedures and add written instructions to the school’s **Local Procedures Manual** ([Model Procedures](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-model-procedures.docx) available)
5. Require staff handling/processing account/card data to complete staff declarations ([Staff Declaration](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-staff-declaration.doc) template available)
6. All staff to sign as evidence of receipt of the PCI DSS Policy ([Staff Log](https://ask.schoolschoice.org/resources/suffolk-schools/finance/pci-staff-log.doc) template available)
7. Complete **the PCI DSS** [**Self Assessment Questionnaire B**](https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-B.pdf?agreement=true&time=1548415465604), the signed copy is retained in school – annual task
 |
| **QUESTION** | **ANSWER** |
| This looks daunting and a lot of work for schools – is it? | The majority of schools will only need to complete the annual Certificate and send it to the Schools’ Accountancy Team.Schools using ParentPay or another 3rd party organisation will also need to check that the 3rd party is following the Payment Card Industry’s Data Security Standards (PCI DSS) – the 3rd party organisations usually provide a Certificate of Attestation on their websitesFor schools who hold and/or process card data/payments there is a lot of work to do this first year as the Self Assessment Questionnaire B must be completed. This will be an annual task but completing the document should be easier after the first year.  |
| What contact details should I use for queries? | Please read through the various documents available (see links on page 1) and the questions and answers contained here as they may contain the answer to your query.If after doing this you still have a query then: * Contact the Schools’ Accountancy Team if it is a question related to what you are expected to do
* If your queries relate to specific questions in the Self Questionnaire B then you will need to use the PCI Security Standards Council’s [FAQ Knowledge Base](https://www.pcisecuritystandards.org/faq/). If these do not provide the answer that you need then there is the facility within the FAQ Knowledge Base to ask additional questions.
 |
| How can we check if the Schools Accountancy Team has received our certificate or compliance? | You can check if we have received your certificate by looking at the [Register of Returns](http://www.suffolklearning.co.uk/leadership-staff-development/schools-accountancy/financial-management/financial-administration) on the Suffolk Learning Website. This document is updated weekly, so there may be a delay between us receiving your document and the register.  |

|  |  |
| --- | --- |
| **QUESTION** | **ANSWER** |
| How should we store the various documents we are required to have?  | The Schools’ Accountancy Team recommend that schools maintain a PCI DSS folder which includes (where appropriate):* The school’s current PCI DSS Policy
* The school’s current Payment Card Handling Procedures
* The PDQ Terminal operating manual and ‘short-cut’ guide
* Evidence that all staff have had access to the school’s PCI DSS Policy and Procedures e.g. PCI DSS Staff Log
* Signed declarations from all members of staff authorised to handle payment card data (including 16-digit primary account number, expiry date, 3-digit security code) and/or PDQ Terminals
* Log of visual inspections of PDQ Terminal
* Completed, signed PCI DSS Self-Assessment Questionnaires
* Signed Certificate of PCI DSS Compliance
* A copy of the Local Authority’s Finance Regulations and copies of appropriate LMS Documents and FAQs

Staff should be aware of where to find the file and any appropriate documents not located in the file.Maintaining a file in this way will also assist audit inspections. |
| How do I obtain an *Attestation of Compliance* from a 3rd-party organisation? | These can normally be found on the 3rd-party provider’s website e.g. [ParentPay](https://www.parentpay.com/Schools/Security-Data-Protection/PCI-compliant-secure-online-payments-for-schools/). If you cannot find the appropriate attestation then you will need to contact the company. If appropriate information is not forthcoming then the school should decide whether it is appropriate to continue to use the 3rd-party organisation. |
| How often will we need to re-do these documents/checks? | The Certificate and Questionnaire will need to be completed annually or earlier if any changes are made such as the location of a TerminalThe timescales for review of the Policy and Procedures will be decided locally by the schoolThe attestation of 3rd-parties should be confirmed each year prior to completing the CertificateCompliance with the Finance Regulations and the school’s Policy and Procedures should be on-going  |
| What needs to be sent to the Schools’ Accountancy Team? | The Certificate needs to be sent to SAT by 31 March. No other documents should be sent unless they are requested. |
| Our school needs to complete the Self Assessment Questionnaire B – do we need to send it anywhere? | You need to complete this annually and retain the signed copies in school.If the LA asks for a copy then you will need to comply with the instructions contained in the request.Audit may ask to see the originals when carrying out an inspection at the school. |